Preliminary Draft Response to System of Systems Focus Group Tasking
Version 05/23/08

In March, the PSRSPC TWG reviewed DGS TD/PSRSPC tasking assigned the 'System of Systems" (SoS) Focus Group with a completion date of September 1st 2008. The following represents a preliminary draft response to this tasking (which tasking is reiterated below):

PSRSPC Direction

1) Develop a definition of what the term "System of Systems" means.

    a) What are the operational characteristics?
    b) With regard to the operational characteristics---do they currently exist in State systems or do they have to be added?
    c) How would the "SoS" perform in one or more scenarios (the San Diego fires and San Francisco Earthquake scenarios come to mind---but also some smaller events, like a major accident on a highway, etc.) to enable State agencies to respond and work together in mitigating the event?

2) Are there technical issues that need to be resolved? If so, what are they?
    a) Can the technical issues be resolved with technology that is currently available in the marketplace? The "SoS Focus Group" is NOT EXPECTED to conduct an extensive search of technology to answer this question.
    b) Is the P25 ISSI an appropriate solution? If not, what is lacking?

3) Are there operational issues that need to be resolved? If so, what are they?
    a) Who should be responsible for developing solutions to these issues? (Probably outside the responsibility area of the "SoS Focus Group")

4) Are there governance issues that need to be resolved? If so, what are they? This should then be passed to the "Governance Focus Group" to resolve.

5) What (specifically) does each of the PSRSPC members need to do within the next two years to enable a "SoS"?
    a) Do they have the resources (staff, equipment, approved budget authority) to do this? If not, it cannot be done.

6) What (specifically) does each PSRSPC member need to do in the 2-5 year timeframe to enable "SoS" between and amongst State agencies? This would become the basis for the development of BCP's, as appropriate.

7) In cooperation with CalSIEC---how can the State's "SoS" be expanded to include interoperability between State agencies and agencies at the county, local, and tribal level?
    a) Can these actions be taken solely by the State, or do they involve action by the county/local/tribal agency?
    b) Provide a "responsibility" matrix.

Some of this (in particular Question #6) would need to be integrated into the "Strategic Planning" effort that will be conducted under the PSIC Grant. It should be pointed out that this would be a "subset" of what the "Strategic Planning" Group is doing since this addresses only the issue of interoperability (the "Strategic Planning" Group should be looking at both "operability" planning and "interoperability" planning---and should be expanding the "view" to 10 years).

REFERENCES

The following overview benefited significantly from, and includes unquoted extracts throughout from, the following U.S. DOJ, DHS SAFECOM, CalSIEC/PSRSPC, and P25 Technology Interest Group website offerings – and some not mentioned due to oversight. The final version will note attributions correctly:

1. U.S. DOJ Law Enforcement Tech Guide for Communications Interoperability: "A Guide for Interagency Communications Projects"
2. Public Safety Statement of Requirements for Communications and Interoperability
3. The California Statewide Communications Interoperability Plan
4. The PSRSPC Annual Report to the California Legislature
5. PTIG P25 Standards Update IWCE2007 Power Point Slides

1. Develop a definition of what the term "System of Systems" means.

OVERVIEW

Interoperability is built up from separately operable systems. It's a defining quality of a system of systems. For example, the modularity and scalability of modern incident command systems mean they are useful from small incidents to large-scale emergencies. Separate command teams can even be folded into one as incidents merge.

Definition of System of Systems

A set or arrangement of independent systems that are related or connected to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole.

The envisioned PSRSPC and/or CalSCIP public safety communications system of systems is a functional collection of people, technology, and business processes.

Strategy

Achieve a system-of-systems environment supported by communications standards, tools, and best practices. Promote a system of systems approach through the use of standards-based communications equipment.

Near-Term Goals

Since communications interoperability is achieved through a system of systems—both technological and operational—needs are many and varied. Project success pivots on meeting well understood and defined needs. Needs analysis feeds acquisition, implementation, maintenance, and most other system development efforts. At a high level, the needs analysis entails:

- Assessing Current Business Processes
- Determining Stakeholder Needs

- Developing General System Requirements
- Evaluating Options

Long-Term Goals

Establish an integrated system-of-systems which is in regular use, allows public safety personnel to communicate (voice, data, and video) with whom they need on demand, in real time, and as authorized.

This long-term goal is compatible with the following:

- **PSRSPC Vision:** *Develop, implement, and administer an innovative, inclusive, scalable, and sustainable statewide plan that facilitates wireless communications system modernization and interoperability and ultimately provides effective, seamless, and reliable public safety services throughout California.*

- **PSRSPC Mission***:* *To provide the leadership needed that allows California to effectively leverage existing investments in communications infrastructures while moving rapidly and decisively to meet targeted goals for improved interoperability, universal statewide access, enhanced modernization, increased functionality, and adequate channel availability throughout California in support of public safety.*

- **CalSCIP Vision**: *By 2017, ensure all local, regional, tribal, state and federal public safety first-responders and designated public service organizations operating within California will be able to communicate in real time, across disciplines and jurisdictions, to respond more effectively during day-to-day operations and major incidents.*

- **CalSCIP Mission:** *Provide a statewide strategic planning framework for an innovative, inclusive, scalable, sustainable, and well-managed interoperability infrastructure that promotes national standards, and is effective in addressing the unique urban and rural requirements of the public safety first responders and designated public service organizations serving the citizens of California.*

PSRSPC-RELAVANCE

System of Systems Concept Defined

System of Systems in this context can be defined as a solution that addresses large-scale, multi-jurisdictional and interdisciplinary public safety communications problems due to the existence of incompatibilities between non-standard public safety agency communications systems and equipment (hereafter “dissimilar distributed systems”). Definitions and views may vary, but it is widely agreed that the concept, System of Systems, is a new discipline of which much still has to be learned. The method or process for addressing SoS challenges are being described as System of Systems engineering.

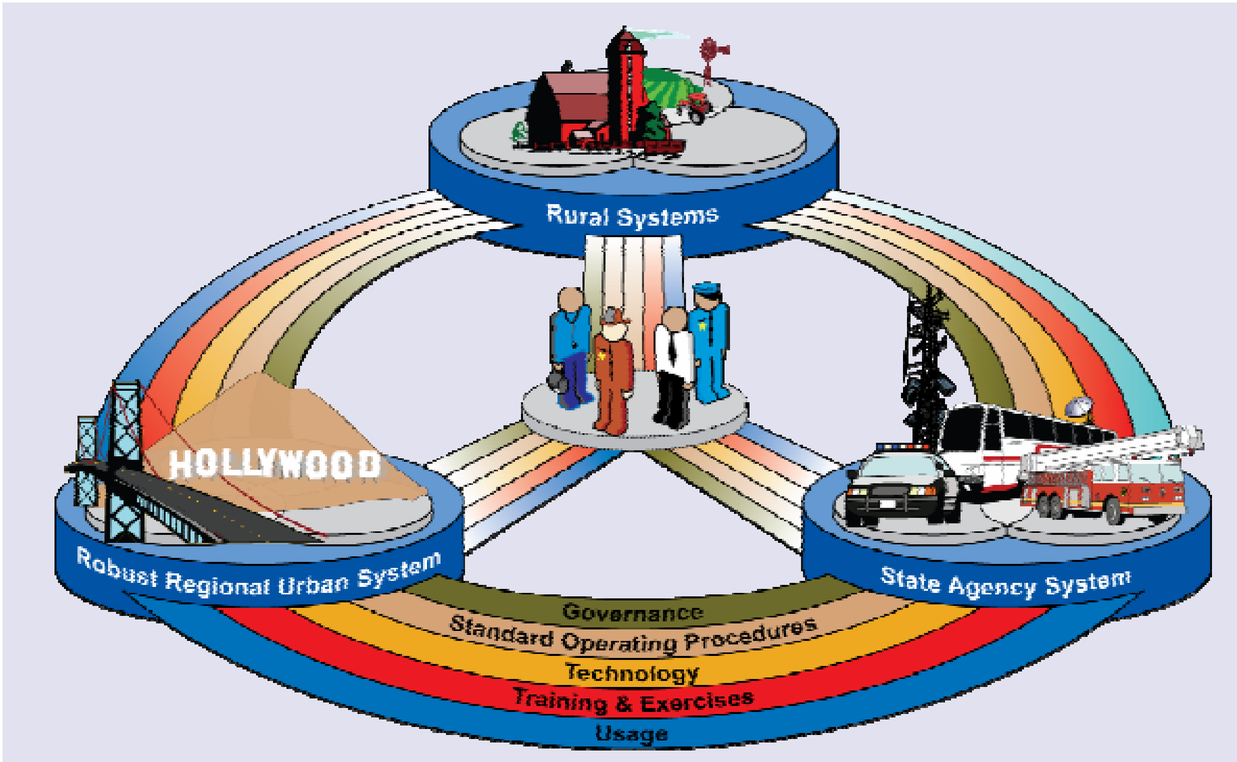
Specifically for California public safety/public service agencies, it is a solution that solves a complex public safety communications interoperability problem due to dissimilar distributed systems by using technology, policy, and economics.

California's Complex Public Safety Radio Communications Problem

Dissimilar distributed systems, policy, and economics combine to form the current state of public safety radio interoperability within California. A System of Systems approach is needed to expose and deliver new ideas. In the context of California's 2017 Vision for achieving state-wide interoperability, an SoS solution includes a state-wide multi-system network that interconnects emergency responders who are operating on separate agency radio systems. This concept helps address the need to retain a level of local and regional autonomy among individual agencies, jurisdictions, and regions that have already built out communications systems. Ultimately, the goal of the SoS concept is to enable direct interoperable radio communications regardless of an agency's jurisdiction or discipline, or the location of the emergencies.

The 2007 CalSCIP identified the three levels of the System of Systems concept as follows*:*

1. Local Response Area system interoperability: interconnection of individual agency systems within a municipality or county.
2. Regional system interoperability: interconnection of individual local response area systems throughout a region. A Region is a defined geographical cluster of individual response areas.
3. Statewide interoperability: interconnection of regions throughout the state.



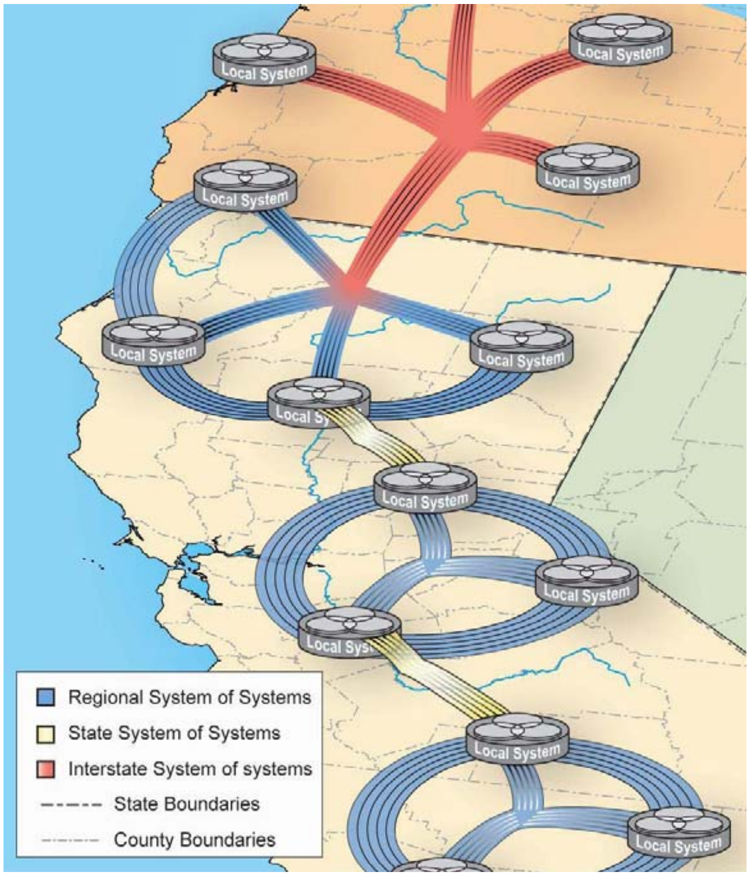
Implications of System of Systems Interconnection (Source: 2007 CalSCIP)

Achieving Interoperability through a System of Systems

The concept for an SoS network architecture is based on technology "hubs," which allow controlled interconnection of individual radio systems; statewide interoperability is achieved by interconnecting hubs. Controlled, shared use of compatible radio systems can be integrated into the hub architecture.

The 2007 CalSCIP indicated that a typical hub concept will include the following:

1. Local Response Area Hub: interconnection of a cluster of individual systems to enable interoperable communications between individual agencies within a Local Response Area, such as a municipality, county, or other local service area boundary.
2. Regional Hub: interconnection of a cluster of Local Response Area hubs within a defined geographic boundary to enable interoperability between emergency responders in different Local Response Areas within a region.
3. State Hub: interconnection of all Regional Hubs to enable statewide interoperability between emergency responders in different regions. The State can work to integrate systems as regional hubs are further developed.



Envisioned System of Systems for California by 2017 (Source: 2007 CalSCIP)

CA State agencies and local governments have already invested time and money in their efforts to remedy ongoing regional communications needs. In many cases, exceptionally effective systems that integrate equipment and procedures have developed over time, which has created discrete interoperable communications neighborhoods around California. However, there is the critical need to link these communications neighborhoods together through standards-based bridging technologies and procedural agreements in order to create a statewide interoperable communications network of these discrete systems (i.e., a “System of Systems”), through which all local, regional, and state entities can communicate seamlessly and effectively.

The SoS concept of connectivity aligns with the objectives outlined in the CalSCIP strategy section. Contributing technologies to the SoS align with various Federal grant requirements by adopting advanced technological solutions to achieve communications interoperability.

Looking into the future, the concept can be expanded to interconnect state hubs between states to enable inter-state interoperability. The specific agency requirements for each individual system are not compromised in the SoS concept, therefore, individual agencies will be able to control their participation in an interoperability connection.

Critical Agency Participation & Next Steps

It is essential that all agencies that operate within the state actively participate in a unified governance structure to ensure the successful implementation of a statewide SoS. The critical first step is *completing* the needs analysis of all communications capabilities among State and affiliate emergency response agencies within the state.

The comprehensive needs analysis will assess current business processes by:

- assessing the interoperability baseline
- defining interagency business processes
- defining the current technology environment
- fixing the (newly) obvious problems
- describing how current technology is used to accomplish work

The needs analysis will determine stakeholder needs through:

- collecting artifacts (formal or anecdotal de facto requirements)
- collecting scenarios (planning, training, exercise, et cetera)
- conducting interviews and focus groups

The needs analysis will then allow for the development of general system requirements through:

- defining general organizational, operational, and technical functional requirements
- defining general interface and integration requirements
- creating a conceptual design

This requirements survey will include all fields required for data analysis using CASM or other accepted databases. Once the current state of communications capabilities is evaluated within California, the next step is to reach out to industry officials as a unified group and request information regarding existing capabilities, services, and technologies that will allow the State to move forward with implementation of the SoS. This can best be achieved through a series of Requests for Information (RFIs).

A standard RFI describes the purpose of the request and outlines the scope of the project or services to be performed. The intent is to allow industry service providers to supply targeted information on a specific topic, in this case, the SoS solutions or technical approaches. This information can help the State's leadership in decision-making and the defining next steps. The format of the RFI should be concise and simple, and should request specific information; this format helps State leaders quickly analyze the responses and leverage the submitted information.

a. What are the operational characteristics?

Define General Functional Requirements

The baseline Wireless Voice Capabilities (seeking Communications Regardless of Technologies, Infrastructures, and Frequency Bands), the Wireless Data Capabilities, and the Information Systems Capabilities the SoS envisions enabling can be found in Attachment "B".

Requirements need to be defined in functional terms and compiled into a report presenting them along with a conceptual design that illustrates how they fit together. The first step in pulling together that report is to compile requirements from preceding work.

Functional requirements are defined in terms of just how the "system of systems" will work to accomplish project goals and meet its vision.

It is important not to allow preconceived "solutions" to slip into the requirements. The price to pay in noncompetitive bids that are challenged is just too high—and may not yield the best solution for meeting the defined operational needs.

Requirements need to be sorted into organizational, operational, and technical categories.

b. With regard to the operational characteristics---do they currently exist in State systems or do they have to be added?

Considering their age and relative degree of non-sophistication, many of the operational characteristics do not exist in today's CA State agency systems.

c. How would the "SoS" perform in one or more scenarios (the San Diego fires and San Francisco Earthquake scenarios come to mind---but also some smaller events, like a major accident

on a highway, etc.) to enable State agencies to respond and work together in mitigating the event?

See Attachments "A" & "C" for examples.

2. Are there technical issues that need to be resolved? If so, what are they?

General Interface and Integration Requirements

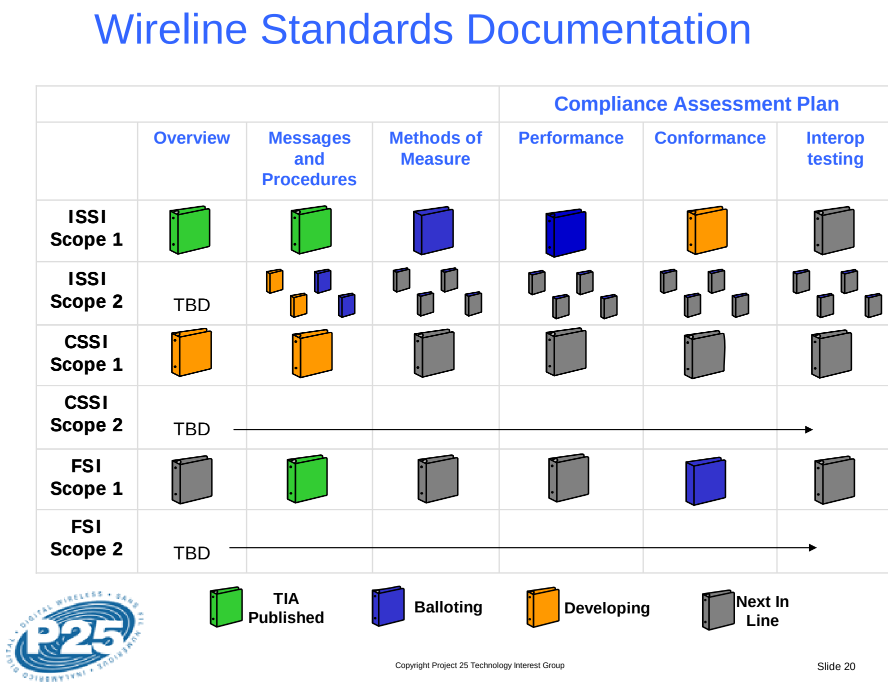
All systems have geographic, functional, and technical boundaries that have to be bridged and every interoperability project has internal points of interface between communications systems and subsystems. Very few projects are initiated to uproot all communications components for all agencies—from voice radios, to backbone networks, to consoles and beyond—so integration of the old with the new is generally inevitable. State agency systems encompass components that won't be replaced in this effort to improve interagency communications. Ideally, they can all be integrated to the extent they can honestly be called a "system of systems."

This step in defining requirements establishes what parts of existing systems will stay and which may go. It defines required points of interface between those that stay and any new technology that may be implemented. This is the place to document specifications that will shape proposed technology solutions.

a. Can the technical issues be resolved with technology that is currently available in the marketplace? The "SoS Focus Group" is NOT EXPECTED to conduct an extensive search of technology to answer this question.

Not all envisioned P25 suite of standards technologies are currently available in the marketplace. Many P25 standards have been completed, published, and their functionality is available through an assortment of manufacturer's offerings. Some are in the development stages (with equipment availability projections unknowable), and for some, development has not yet begun.

For example, P25 wireline standards are still in various states of development as indicated in the "Wireline Standards Documentation" figure below.



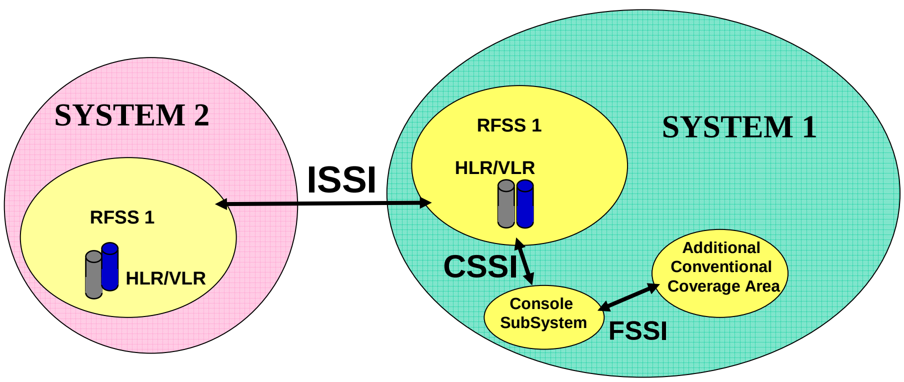
The Project 25 Document Suite Reference at http://www.its.bldrdoc.gov/resources/p25/P25DocSelection.pdf tracks the current state of Project 25 standards documents. The Telecommunications Industry Association (TIA) TR8 Committee meets quarterly to develop, revise, and approve Project 25 standards documents. This document is updated soon after each TR8 Committee meeting to reflect Project 25 standards document progress.

b. Is the P25 ISSI an appropriate solution? If not, what is lacking?

The ISSI is an open IP-based interface relying on standard IP protocols for voice transport using Real-time Transport Protocol [RTP] and signaling using Session Initiation Protocol [SIP].

The Inter RF Subsystem Interface (ISSI) affords the following connectivity:

ISSI, Fixed Station Subsystem Interface and Console SubSystem Interfaces



ISSI Inter Sub System Interface
FSSI Fixed Station Subsystem Interface (conventional interface)
CSSI Console Sub System Interface
HLR Home Location Register (manages home subscribers)
VLR Visitor Location Register (manages visitor subscribers)
RFSS Radio Frequency Sub System

Slide 18

Wireline Interface Scope definitions

- **ISSI**
  - **Scope 1**
    - Trunked Talkgroup call, Unit to Unit call (Individual), Mobility (Subscriber roaming) and Authentication
  - **Scope 2**
    - Conventional, Data, OTAR (Over The Air Rekeying), Console across ISSI, Supplementary data (call alert, etc.)
- **Fixed Station Interface**
  - **Scope 1**
    - Voice & Station control for analog/P25 air interface supported over 4-wire (analog) and Ethernet (digital) transport between console and single fixed station.
- **Console Subsystem Interface**
  - **Scope 1**
    - Uses the Trunked ISSI features and incorporates Conventional ISSI features.

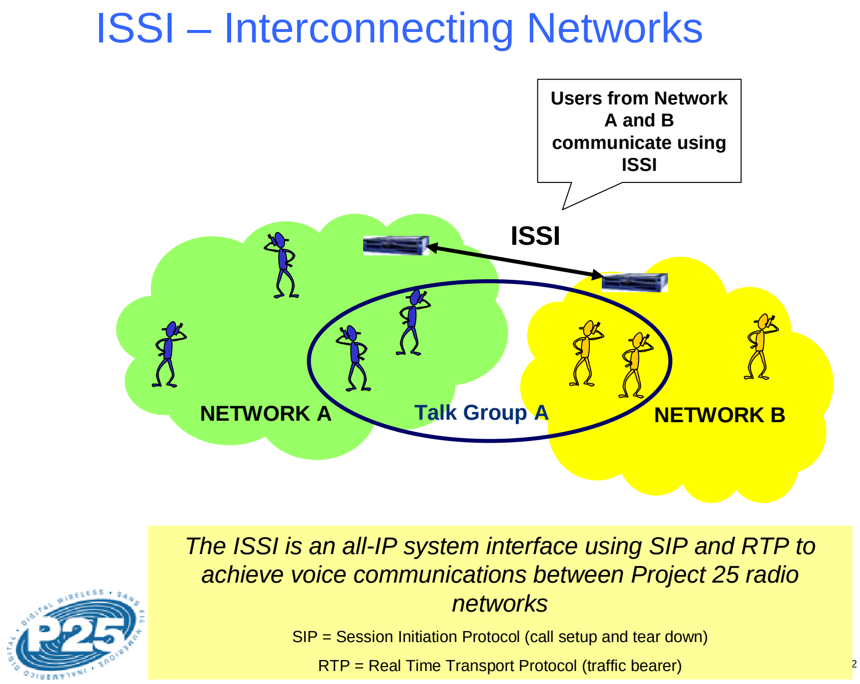
Slide 19

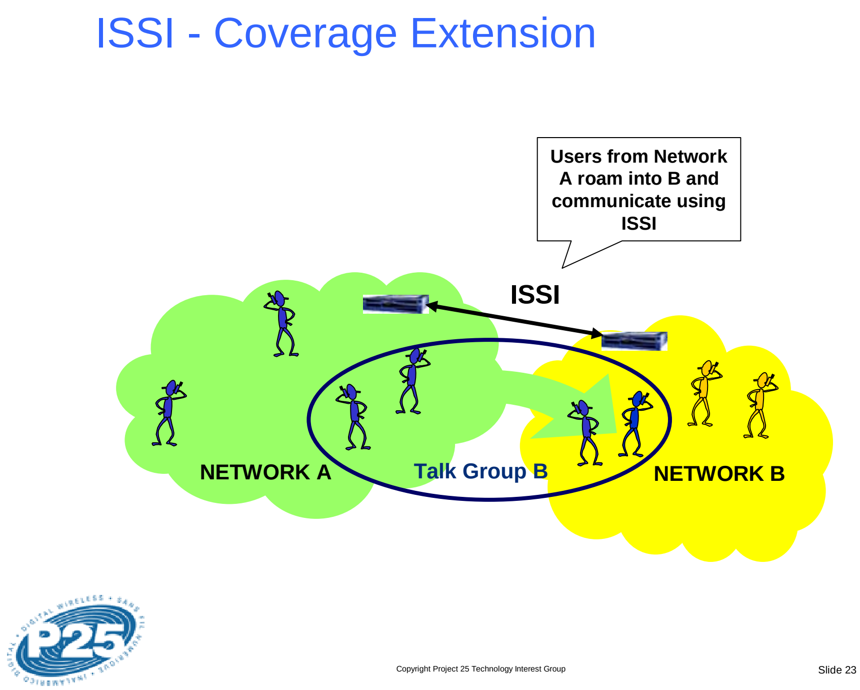
In the absence of having performed a comprehensive interoperability needs analysis, the Inter RF Subsystem Interface (ISSI) appears to address all the rudimentary requirements of interoperability.

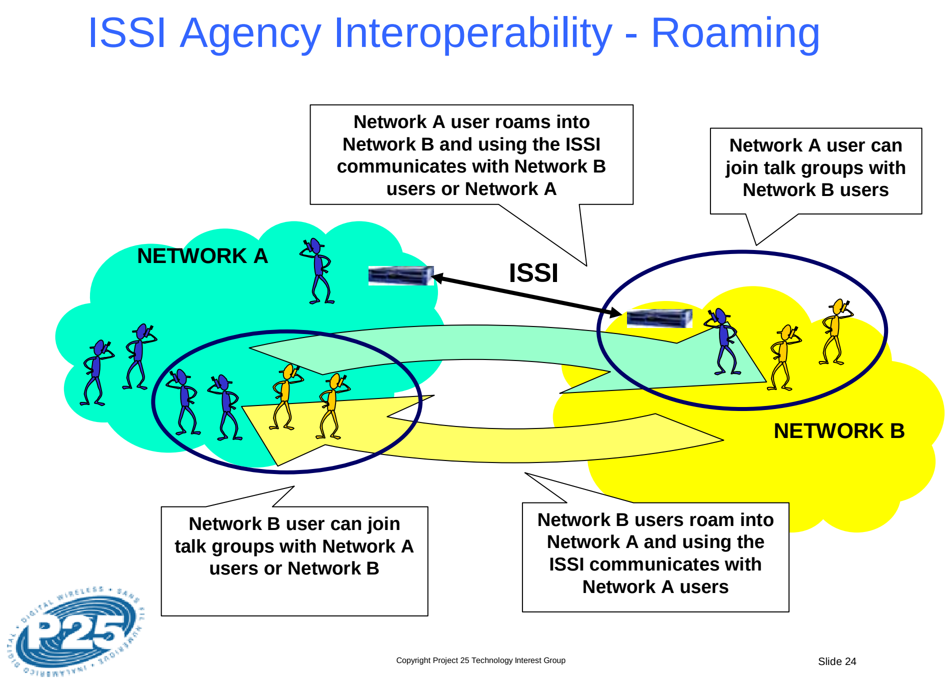
That is, the ISSI enables:

- Authentication of roaming radios
- Tracking current location of roaming radios (subscriber database management)
- Voice transport
- Project 25 addressing scheme
- Unit/Group Call setup & teardown
- Home-based PTT services to roaming radios
- PTT communications management among roaming and home-based radios

This allows for the following types of interoperable communications:







3. Are there operational issues that need to be resolved? If so, what are they?

The magnitude and specificity of the operational issues to be resolved will be fully revealed after the needs analysis for each agency is completed. This is underway and will entail each agency completing its current and projected:

- intra-agency (operability) needs analysis, and
- interagency (interoperability) needs analysis

Analysis of the combined results for each agency, and the correlating results of all other agencies, will uncover the operational issues needing resolution. These "issues" may show up in various forms; examples include:

- the projected intra-agency and/or interagency practices is not supportable by available or projected technological solutions, or
- an agency's current and/or projected interagency interoperability practices are in conflict with another correlating agency's current and/or projected interagency interoperability practices.

a. Who should be responsible for developing solutions to these issues? (Probably outside the responsibility area of the "SoS Focus Group")

Each affected agency will likely choose to augment its current and/or projected intra-agency operational issues to synchronize with best practices, available solutions, et cetera.

Each affected agency may choose to augment its current and/or projected interagency operational issues to synchronize with best practices, available solutions, et cetera. Since State agency interoperability issues are the purview of the PSRSPC, guidance from the PSRSPC and its Technical Working Group will be invoked as necessary.

4. Are there governance issues that need to be resolved? If so, what are they? This should then be passed to the "Governance Focus Group" to resolve.

The magnitude and specificity of the governance issues to be resolved will be fully revealed after the needs analysis for each agency is complete and analyzed. This is underway and will entail each agency completing its current and projected:

- interagency (interoperability) needs analysis.

Analyses of the combined results for each agency, and the correlating results of all other agencies, will uncover the governance issues needing resolution. These "issues" may show up in various forms; examples include:

- an agency's current and/or projected interagency governance practices are in conflict with another correlating agency's current and/or projected interagency governance practices.

Each affected agency may choose to augment its current and/or projected interagency governance issues to synchronize with best practices, available solutions, et cetera. Since State agency interoperability issues are the purview of the PSRSPC, guidance from the PSRSPC and its Technical Working Group will be invoked as necessary.

5. What (specifically) does each PSRSPC member need to do within the next two years to enable a "SoS"?

Prior Proper Planning Prevents Poor Performance. Within the interval from now until June of 2010, several activities need to be underway. The generation of a strategic plan, the performance of a needs analysis, and the completion of outstanding Annual Report issues.

The ideal path is to improve operability *and* interoperability simultaneously. For example, if an agency needs additional portables to meet their basic operability needs, P25 equipment should be purchased to augment the transition towards interoperability. In fact, CA Government Code 8592.5 requires the purchase of P25-compliant radio communications equipment.

Within the next two years (through June, 2010), agency-projections of work each agency intends to perform are reflected below:

AGENCY	PROJECTED AGENCY EFFORTS THROUGH JUNE 2010						
	Agency Contribution to Development of Strategic Plan	Perform Intra-agency Needs Analysis	Perform Interagency Needs Analysis	PSRSPC Initiative Support	CalSIEC Initiative Support	Other:	Agency-specific Technology Upgrades or Enhancements (Please Describe)
CALFIRE	X	X	X	X	9;12		
CALTRANS	X	X	X	X	9;12; 13		
CDCR	X	X	X	X	9;12		
CHP	X	X	X	X	9;12		
CMD	X	X	X	X	9;12		
DFG	X	X	X	X	9;12		
DGS	X	X	X	X	5-9; 12;13		
DOF	?	?	?	?	?		
DOJ	X	X	X	X	9;12		
DPH	X	X	X	X	9;12		
DPR	X	X	X	X	9;12		
DWR	X	X	X	X	9;12		
EMSA	X	X	X	X	9;12		
OES	X	X	X	X	1-16		
OHS	X	X	X	X	X		

Note: X indicates OHS will support other agencies in their endeavors as an advocate

Do they have the resources (staff, equipment, approved budget authority) to do this? If not, it cannot be done.

AGENCY	PROJECTED AGENCY EFFORTS THROUGH JUNE 2010						
	Agency Contribution to Development of Strategic Plan **Staff/Budget/Equipment**	Perform Intra-agency Needs Analysis **Staff/Budget/Equipment**	Perform Interagency Needs Analysis (TICP derivative) **Staff/Budget/Equipment**	PSRSPC Initiative Support **Staff/Budget/Equipment**	CalSIEC Initiative Support **Staff/Budget/Equipment**	Other:	Agency-specific Technology Upgrades or Enhancements (Please Describe) **Staff/Budget/Equipment**
CALFIRE	Y/Y/NA	Y/Y/NA		Y/N/NA			
CALTRANS	Y/Y/NA	Y/Y/NA		Y/N/NA			
CDCR	Y/Y/NA	Y/Y/NA		Y/N/NA			
CHP	Y/Y/NA	Y/Y/NA		Y/N/NA			
CMD	Y/Y/NA	Y/Y/NA		Y/N/NA			
DFG	Y/Y/NA	Y/Y/NA		Y/N/NA			
DGS	Y/Y/NA	Y/Y/NA		Y/N/NA	Y/N/NA		
DOF	?	?	?	?	?		
DOJ	Y/Y/NA	Y/Y/NA		Y/N/NA			
DPH	Y/Y/NA	Y/Y/NA		Y/N/NA			
DPR	Y/Y/NA	Y/Y/NA		Y/N/NA			
DWR	Y/Y/NA	Y/Y/NA		Y/N/NA			
EMSA	Y/Y/NA	Y/Y/NA		Y/N/NA			
OES	Y/Y/NA	Y/Y/NA		Y/Y/NA	Y/Y/NA		
OHS	X	X	X	X	X		

6. (a) What (specifically) does each PSRSPC member need to do in the 3-5 year timeframe to enable "SoS" between and amongst State agencies? This would become the basis for the development of BCP's, as appropriate.

AGENCY	PROJECTED AGENCY EFFORTS JULY 2010 THROUGH JUNE 2013						
	PSRSPC Initiative Support	CalSIEC Initiative Support	Other:	Other:	Other:	Agency-specific Technology Upgrades or Replacements (Please Describe)	State-to State Interagency Technology Upgrades or Replacements (Please Describe)
CALFIRE	X						
CALTRANS	X						
CDCR	X						
CHP	X						
CMD	X						
DFG	X						
DGS	X	X					
DOF	?	?					
DOJ	X						
DPH	X						
DPR	X						
DWR	X						
EMSA	X						
OES	X	X					
OHS	X	X					

Note: X indicates OHS will support other agencies in their endeavors as an advocate

6. (b) What (specifically) does each PSRSPC member need to do in the 6-10 year timeframe to enable "SoS" between and amongst State agencies?

AGENCY	PROJECTED AGENCY EFFORTS JULY 2013 THROUGH JUNE 2017		
	Agency-specific Technology Upgrades or Replacements (Please Describe)	State-to State Interagency Technology Upgrades or Replacements (Please Describe)	Other:
CALFIRE			
CALTRANS			
CDCR			
CHP			
CMD			
DFG			
DGS			
DOF			
DOJ			
DPH			
DPR			
DWR			
EMSA			
OES			

AGENCY	PROJECTED AGENCY EFFORTS JULY 2013 THROUGH JUNE 2017		
	Agency-specific Technology Upgrades or Replacements (Please Describe)	State-to State Interagency Technology Upgrades or Replacements (Please Describe)	Other:
OHS			

7. In cooperation with CalSIEC---how can the State's "SoS" be expanded to include interoperability between State agencies and agencies at the county, local, and tribal level?
    a. Can these actions be taken solely by the State, or do they involve action by the county/local/tribal agency?
    b. Provide a "responsibility" matrix.

There are potentially two classes of State to non-State CalSIEC Interoperability requirements – affiliated (i.e., non-State agencies currently affiliated with State agencies through formal or anecdotal interoperability agreements) and unaffiliated (i.e., non-State agencies lacking any demonstrated State/non-State interoperability correlation). However, since the CalSCIP objective is to *"…establish an integrated system-of-systems which is in regular use, allows public safety personnel to communicate (voice, data, and video) with whom they need on demand, in real time, and as authorized….",* it appears we need to assist in determining potential interoperability correlations between State and currently unaffiliated, non-state public safety agencies. It also appears the CalSCIP provides the PSRSPC and/or CalSIEC-represented agencies with justification to seek Federal support in advancing the State's ability to interoperate with traditional non-State affiliates, and with former non-affiliates where a need for interoperable communications can be demonstrated.

The chart below is a preliminary pass at creating a responsibility matrix for perceived task development.

AGENCY	PROJECTED STATE AGENCY COLLABORATIVE EFFORTS THROUGH JUNE 2017			
	Perform Interagency Needs Analysis	**Assist in Determining Potential State Interoperability Correlations with currently unaffiliated, Non-State bona fide Public Safety agencies**	**Collaborated State/Local/Tribal/Federal Interagency Technology Upgrades or Replacements**	**Other:**
Affiliated, Non-State Public Safety	X	N/A		
Unaffiliated, Non-State Public Safety	X			
CALFIRE	*			
CALTRANS	*			
CDCR	*			
CHP	*			
CMD	*			
DFG	*			
DGS	*			
DOF	*			
DOJ	*			
DPH	*			
DPR	*			
DWR	*			
EMSA	*			

AGENCY	PROJECTED STATE AGENCY COLLABORATIVE EFFORTS THROUGH JUNE 2017			
	Perform Interagency Needs Analysis	Assist in Determining Potential State Interoperability Correlations with currently unaffiliated, Non-State bona fide Public Safety agencies	Collaborated State/Local/Tribal/Federal Interagency Technology Upgrades or Replacements	Other:
OES	*			
OHS	*			

* Interagency analyses already performed for affiliated, non-State public safety agencies from a State perspective; Non-State agencies have a requirement to develop rudimentary Tactical Interoperable Communications Plans (TICP's) by the end of 2008 wherein their interoperability needs with the State may be defined to some extent. State agencies may choose to take a lead role in "assisting" those non-State agencies who lack the resources and/or perspective to envision the real or potential need for interoperability with State agencies.

ATTACHMENT "A"

Extract from U.S. DOJ "Law Enforcement Tech Guide For Communications Interoperability"

FACTS:

• Interoperability is achieved when services are delivered seamlessly across organizational subdivisions and between jurisdictions.

• An enterprise view of public safety services—for example, across a city, county, or metropolitan region—uses a citizen-centered, results-focused definition of services provided to define, among other things, necessary interagency information exchanges.

• With services and these interagency junction points defined, a technological framework can be built that leverages existing investments and capabilities, reduces redundancies, and establishes de facto standards for future systems.

• Both services and supporting systems have to be integrated for the public safety enterprise to have communications interoperability.

A Complex System of Systems

Modern agencies have a staggering array of systems supporting their services. How complex? Consider a typical call that's handled thousands of times each day across the country: A landline telephone call reporting a motor vehicle accident with injuries.

The Call Arrives

From the 9-1-1 call, an automatic call distributor may first direct the connection to an open attendant position, providing automatic number identification (ANI) information from the call. In the background, call-logging recorders track the source, routing, and conversations. An instant playback recorder may begin to capture the conversation for the operator's subsequent use while an audio logging recorder elsewhere makes a more permanent record. Where enhanced 9-1-1 (E9-1-1) is available, the caller's address is automatically retrieved and provided to the operator. The call to the public safety answering point (PSAP) is then either dispatched by the operator or transferred to a dispatcher across the room or perhaps even across town. And that's all before response is initiated. E9-1-1, ANI, ALI, PSAP, MSAG... there's certainly no shortage of acronyms in the public safety communications business! Wait, there's more.

The Call is Dispatched

If the call-taker hasn't already done so, the incident might automatically be queued to a computer-aided dispatch (CAD) system at this point—or maybe even separate CAD systems for fire medical and police response. The CAD system itself is a complex animal. From this point, it may interface through a general purpose console with telephone, alarm, paging, voice radio, mobile data, and logging systems. It might be fed mapping information in the background for geographic display of call source, responder location, and street closure indications. For later use, it might feed incident information to an agency's records management system (RMS) or simply drive a run card printer in a distant fire station.

First Responders Respond

From dispatch, let's imagine that fire medical responders are alerted by a page and police officers by a message sent wirelessly to the squad car's mobile data computer. Fire paramedics grab the run card, jump in their vehicle, and transmit acknowledgment of the call over a voice radio system. By way of a couple of key presses, the police officer acknowledges receipt of the alert and notifies dispatch of an impending response with lights and siren. En route, automatic vehicle location (AVL) systems in each unit transmit current location information to dispatch from a Global Positioning System (GPS) receiver for display on a geographic information system (GIS)-powered map in dispatch. On scene, the officer quickly transmits an arrival status message and turns to a shared radio channel to direct paramedics in from an alternate direction because the roadway is blocked by backed-up traffic.

Service is Delivered

Response is well underway, with a great deal of technology enabling it. A transporting ambulance may have been dispatched by this point and street maintenance alerted to divert traffic around the accident. Medical control may have been established through a nearby hospital and its emergency room notified of the impending arrival of patients. More systems are tied in. Eventually patients are delivered, cars towed, accident and run reports filed, and responders returned to routine duties.

This complex system of emergency services is linked through an integrated mesh of communications and information systems.

The hapless victims of our hypothetical accident don't know—and probably don't care at the time—about all that goes into delivering emergency services to them. All they know is that they need help. All the policies, procedures, skills, and technologies that are involved in delivering effective emergency response need to come together at that moment, and at that spot.

ATTACHMENT "B"

Note: Comprises extracts from SAFECOM/ Advanced Generation of Interoperability for Law Enforcement (AGILE)/NIST Summit on Interoperable Communications for Public Safety, held at the National Institute of Standards and Technology (NIST).

Wireless Voice Capabilities

Communications Regardless of Technologies, Infrastructures, and Frequency Bands

Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions, some of which may use different technologies, infrastructures and/or frequency bands regardless of system. Includes the transitioning between commercial systems and private land mobile radio (LMR) systems.

1. Communication with Own Jurisdiction: Ability to communicate with members of own agency/jurisdiction while using the infrastructure of another agency/jurisdiction.

2. Communication with Other Jurisdictions: Ability to communicate with other agencies/jurisdictions using the infrastructure of that agency/jurisdiction.

3. One-to-One Communications: Ability for users to transparently communicate, as authorized, with members of other agencies/jurisdictions on a unit-to-unit (one-to-one) basis.

4. One-to-Many Communications: Ability for users to transparently communicate, as authorized, with members of other agencies/jurisdictions on a unit-to-group (one-to-many) basis.

5. Communications Outside Wireless Infrastructure Coverage: Ability to provide direct communications (talk around) between user radios where wireless infrastructure is unable to support communications (such as in some rural areas, underground parking garages, tunnels, and inside some buildings).

6. Jurisdictional Signal Coverage: Ability to provide jurisdictional-wide signal coverage to system users; optionally, provide ways to enhance or improve jurisdictional coverage in rural areas, underground parking garages, tunnels, and inside buildings that are usually not sufficiently covered.

7. Identification and Authorization: Ability to initiate wireless voice communications by requiring the user to enter (on his/her radio) a user identification that authenticates and validates the user and loads the user's profile. This profile defines talk groups for the user and completes all radio network administration for the user's voice

communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.

8. Priority Levels for Access and System Use: Ability of the agency/jurisdiction to administer the priority for voice communications of particular users and particular public safety applications (such as task force operations and incidents).

9. Emergency Voice Communication: Ability to communicate an emergency voice message (e.g. after pressing a panic button) that has priority over other voice communications.

10. Emergency Signal: Ability to broadcast an emergency signal (e.g. via a panic button) that has priority over other communications.

11. Secure Communications: Ability to have secure (encrypted) voice communications to fit user environment and that satisfy applicable laws, regulations, and policies of the user agencies and jurisdictions.

12. System Administration: Ability to effectively initiate and sustain flexible and dynamic system administration for purposes of multi-agency interoperability, including administration of talk groups, encryption key management, emergency alerts, networks, and channels for mutual aid.

13. Remotely Reprogram User Radios: Ability to remotely (over-the-air) re-program a radio's parameters (i.e., frequency channels, talk groups, squelch control, encryption keys, etc.) and/or modify functionality (e.g., encryption algorithms, waveforms, etc.)

14. Resilient Operations: Ability to sustain resilient operations including tolerance to individual system failures, redundant coverage from adjacent sites, resistance to impact of catastrophic events, etc.

15. Reliable System Performance: Ability to maintain reliable system performance over disparate interconnected systems.

Wireless Data Capabilities

1. On-Scene Wireless Data Networks: Ability to quickly and transparently establish and maintain on-scene wireless data networks (e.g., on scene in a building).

2. On-scene Exchange of Data: Ability of on-scene personnel to transparently exchange data.

3. High-Speed Data Transfer: Capability of high-speed data transfer with ability to sustain performance at network interconnections.

4. Communication with Own Jurisdiction: Ability to exchange data with members of own agency/jurisdiction while using the infrastructure of another agency/jurisdiction.

5. Communication with Other Jurisdictions: Ability to exchange data with members of other agencies/jurisdictions using the infrastructure of that agency/jurisdiction.

6. Sensor Networks: Ability to exchange data involving sensors (e.g., biometric, environmental, personnel location).

7. Identification and Authorization: Ability to initiate wireless data communications by requiring the user to enter (on his/her terminal/radio) a user identification that authenticates and validates the user and loads the user's profile. This profile defines data resource capabilities for the user and completes all radio network administration for the user's data communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as previously authorized.

8. System Administration: Flexible and dynamic system administration (includes administration of wireless data networks, adding users, giving permissions, etc.).

9. Data Security: Ability to ensure secure exchange of information.

10. Information Protection: Ability to protect information according to applicable laws and statutes.

11. Resilient Operations: Ability to sustain resilient operations, including tolerance to individual system failures, redundant coverage from adjacent sites, resistance to impact of catastrophic events, etc.

12. Reliable System Performance: Ability to maintain reliable system performance over disparate interconnected systems.

Information Systems Capabilities

1. Rapid Information Source Access: Ability to provide the exchange of information in a timely fashion to support critical decision points from both field and base locations, including, but not limited to, information regarding identification (photographs, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, computer-aided dispatch (CAD) information, building diagrams, building sensors, transportation information, etc.).

2. Query/Access Multiple Data Sources with One Request: Ability to query/access multiple data sources using one request that is routed to multiple entities simultaneously.

3. “Enter Once—Reuse Forever” Approach to Data Gathering: Ability to enter validated information once and then share and reuse that information among authorized entities.

4. Data Exchange with Computer-Aided Dispatch: Ability to exchange information with CAD and Record Management Systems (RMS).

5. Data Access to Logistical Resource Information: Capability to obtain logistical resource information on all personnel and equipment responding to an incident.

6. Emergency Notifications: Ability to broadcast critical information by means such as text messaging to multiple organizations

7. Formatting: Ability to effectively and efficiently exchange data between agencies/jurisdictions (e.g., by employing common data representation structures and exchange formats and protocols).

8. Open Source Formatting: Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by encouraging open source format.

9. Data Security: Capability of maintaining the security requirements of any entity within a broader security framework.

10. Field Image Capture and Distribution: Capability of field image capture and distribution.

11. Data Access to Background Information Sources: Ability to access information related to hazardous materials, water sources, floor and building plans, fire pre-plans, utility maps, weather forecasts, topographic terrain, transportation, and other background data to support public safety incident management.

12. Data Access to Medical Information: Ability to manage medical information.

13. Data Access to Legal Information: Ability to access legal information, such as investigation/litigation records, court scheduling records, disposition data, and charge data.

ATTACHMENT "C"

Scenario: Earthquake

Outline

1. Scenario Initiation: A 7.2-magnitude earthquake hits Central City.
2. The State Warning Center begins automated notifications.
3. The Public Safety Answering Point (PSAP) receives continuous calls.
4. PSAP dispatches first responders and alerts Emergency Management; helicopters are requested.
5. The EOC is activated.
6. Fire response and EMS arrive at scenes.
7. Radio Amateur Civil Emergency Service (RACES) begins providing communications support.
8. The Mayor notifies the Governor.
9. A unified command is formed onsite.
10. Urban search and rescue (US&R[1]) team and community emergency response teams (CERT[2]) are requested.
11. Central City requests county and state resources; the state mutual aid system is activated.
12. RACES assist outlying areas in the reporting of damages.
13. Staging areas are defined.
14. The Governor activates the National Guard and requests Federal assistance.
15. A conference call is held to identify additional resources requirements.
16. A JIC formed.
17. The state US&R arrives.

[1] An Urban Search and Rescue (US&R) team is a task force, complete with necessary tools and equipment, and required skills and techniques for the search, rescue, and medical care of victims of structural collapse.

[2] Community Emergency Response Teams (CERT) are trained civilian volunteer auxiliary responders that assist victims and provide support for professional responders during a major disaster.

18. CERT Communication Team sets up.

19. The Red Cross establishes shelters, and public bus systems are commandeered for disaster support.

20. The DMAT team arrives; the coroner establishes a body collection and processing center.

21. The CERT Team provides information.

22. Structural specialists survey garage beneath damaged building.
23. Structural specialists warn of a potential building collapse.

24. Search team looks for victims.

25. A gas main has broken, the area is cordoned off.

26. Search teams enter the affected building; DMAT consults with other medical specialists.

27. The operational period ends; the IC rotates the team.

28. National Guard units begin arriving.

29. A Federal US&R team arrives.

Narrative

Santa Luisa County encompasses an area of about 2,800 square miles, bisected by the Santa Luisa Mountains. The county has a population of about 450,000. There are four incorporated cities (Central City, Fernwood, and Otsego on the southeast side of the mountains, and Cooney on the north side). There are two airports—Cooney Regional Airport (the former Cooney Air Force Base), and Santa Luisa Airport at Otsego. It is a summer weekday. At 9:00 a.m. the temperature at Santa Luisa airport was 80 degrees with a slight wind.

An earthquake of magnitude 7.2 hits the Central City area at 9:02 a.m., at the end of "rush hour." Damage to buildings and infrastructure is severe. Utilities are disrupted throughout the city and outlying area. The Cooney Canyon Nuclear Power Plant (CCNPP), located 11 miles outside of Cooney, suffers moderate damage, and requires an emergency shutdown of the plant and the declaration of a site area emergency. Damaged power lines ignite a number of brush fires in the mountains between the CCNPP and Central City. Ruptured natural gas lines lead to a number of residential structure fires. Ground-based, wire and fiber communications to the outside world are temporarily disrupted, and lines within the city, where operational, are immediately overloaded by calls from telephones that were knocked off the hook by the earthquake's shaking and by attempted calls by residents. Restoration of dial tone initially takes many minutes because of this overload. The 911 system remains fully operational due to the telephone company tandem switch into the PSAPs. However, many subscriber cables have been damaged, and the system as a whole suffers from the overload. The 911 system will be severely taxed for the first 12 hours, with only about 1 of 100 callers able to connect to the Central City PSAP.

The cellular system remains minimally operational, although the disruption to long-distance service generally prohibits calls outside of the city. The disruption to ground-based circuits leaves many tower sites isolated and out of service. Mobile-to-mobile calls within each cellular system function properly within areas served by operational towers, although circuits quickly overload from heavy traffic. Cellular 911 trunks linking the Mobile Switching Office to the PSAP remain operational. Thus cellular 911 calls are a significant source of information reaching the PSAP from public callers, particularly at the scenes of some of the major damage. As the incident proceeds, additional cell sites drop off the air as the site battery systems are depleted due to the loss of commercial power.

The county-wide microwave system, designed to withstand an event of this magnitude and linking all trunked public safety radio sites throughout Santa Luisa County, remains fully operational, including the dedicated private automatic branch exchange (PABX) switch that links all of the 911 PSAPs and public safety dispatch centers. The public safety radio system remains operational, as do communications with all mobile and portable subscriber units not damaged by the event. Additionally, at the county seat, the Santa Luisa County EOC has a ground station that is part of a statewide, satellite-based network operated by the Governor's Office of Emergency Management (OEM). This system provides a T-1 equivalent data circuit to Santa Luisa County that can be used for voice telephony, FAX, data, or video conferencing circuits. All are routed through a dedicated switch at the state EOC backed by a redundant switch at the alternate state EOC.

City, county, and state EOCs are equipped with integrated situational information systems designed to provide eagle-eye views of the overall incident as appropriate for that level of management, with the ability to drill down on any specific event or location to show details of the response to and management of it. This information can be shared in real time with field command posts, as well as with responding state and Federal resources. Through this integrated system, information can be retrieved from, and pushed to, the field units. This information system also gives resource managers the ability to monitor, query, and control resources at staging areas, as well as individual assets, in real time.

> ***Note: Electronic communications among all of the personnel involved in this incident are authenticated. For local, on-duty personnel, this authentication takes place when each radio or computing terminal is initially logged on. For personnel responding from other local, state, and Federal jurisdictions, the authentication takes place at the time the unit initially joins the incident, and as different databases are queried or additional communications links established. A regional database processes the authentication of personnel from outside agencies.***

This scenario depicts the first 12 hours of Federal, state, county, and local public safety operations in response to this event.

9:02 AM

1. The local 911 PSAP immediately initiates internal operational and safety checks, noting it is operating on generator power with about 8 hours of fuel. As part of this effort, firefighters and building inspection personnel are dispatched to the PSAP. As the safety checks proceed, investigators use PSCDs to annotate areas of concern on building layout diagrams.

2. The nature of the event automatically activates the city EOC located in the police department immediately adjacent to, but separate from, the city PSAP in accordance with the city's All-Hazard Emergency Management Plan (EMP). The county EOC, located across the street from the city EOC, is automatically activated. The Regional Hospital Patient Management System is automatically activated, and communications links between hospitals are tested to ensure operability.

3. City and county public safety management personnel, many of whom were already at work, and other key city and county staff and volunteers who are assigned to the EOCs begin making their way to the centers. Staff includes members of the public works departments and local public utility representatives. They will track much of the disruption to gas, electricity, sewer, and water systems using a real-time geographic information system (GIS)-based system in the city and county EOCs. The nature of the event also causes automatic call-back of all off-duty city and county personnel. Call-back confirmations are made via voice radio or PSCDs as off-duty personnel begin responding. However, disruption to roads and the light rail system will delay many of these persons from reaching the EOCs for several hours.

4. In Capital City, an automated sensor system has detected the seismic event. The preliminary calculated magnitude of 7.0 causes a number of immediate and automated actions at the SWC operated by the OEM. Actions are based on a series of preprogrammed instructions for this type of event:
   - With a single “approval” entry to the OEM's CAD system, the state EOC is automatically activated, with computer-generated text paging alerts being transmitted across the state to state personnel via a number of commercial paging services. Automatic alerts are also sent to county and local officials and to staff and volunteers within a 100-mile radius of the calculated epicenter of the earthquake. The transmission of these notifications activates the state mutual aid system. Notification confirmations are made via telephone and PSCDs as personnel begin responding.
   - The SWC operator immediately contacts the control terminal for the National Warning System (NAWAS) headquartered at the FEMA operations center outside of Washington, DC. NAWAS is a wire-based, tie-line system linking all 50 states and major Federal Government facilities, including the Department of Defense. This alert is heard simultaneously by all of these facilities, many of whom initiate a preplanned call-up of personnel. Two centers monitoring this initial alert are the regional and national headquarters for FEMA. This alert begins a sequenced notification process to disaster personnel across the country who may be needed.
   - The SWC operator then notifies by telephone the Governor's staff, key legislators, and directors of all state public safety, resource and transportation agencies.

9:10 AM

5. The local 911 PSAP center responds to continuous emergency calls originating from cellular handsets and the few operating wireline telephones in the city. Observers state that a 10-story and a 14-story office building have collapsed, and a Federal building is near collapse. Many other buildings have sustained damage but appear to be structurally sound. Many people are reported injured. The strong odor of natural gas in the downtown area, indicating the possibility of a gas explosion, is also reported. Reports of smoke in residential areas are received from citizens.

6. The PSAP dispatchers initiate first response to the various scenes by alerting the nearest available police, fire response, and EMS units. Fire units, following the CCFD's established seismic event response procedure, report the locations of structure fires on their PSCDs as they survey their initial response districts. The city's Mobile Command Center (MCC) is readied for deployment. The Emergency Manager also requests that state police helicopters be deployed to provide airborne video of the area; the helicopters are equipped with forward-looking infrared (FLIR) cameras enabling them to scan for hotspots indicating surface fires. The county PSAP, operated by the Santa Louisa Sheriff's Department (SLSD) dispatch, receives a call from the SWC via the satellite telephone requesting a preliminary damage assessment for forwarding to state and Federal agencies.

9:15 AM

7. The Emergency Manager, Mayor, and key city staff arrive at and activate the EOC to provide support to the IC and to coordinate the city's resources. Simultaneously, the county's Emergency Manager, County Executive, and key staff activate the county EOC to coordinate the response in the unincorporated areas to the CCNPP site area emergency, and to coordinate information flow and resource allocation to the incorporated jurisdictions within Santa Luisa County.

9:20 AM

8. Although hampered by disrupted roadways and debris, EMS, fire response, and police units respond to the various scenes. Injured persons who can be self-extricated, or easily extricated, are removed from the rubble and collected for transport to treatment centers. Assistance is offered to public safety personnel by many citizens who are now stranded at work sites. All patient names, medical conditions, receiving hospitals, etc. are entered into the EMS unit PSCDs to track the earthquake victims. Additionally, "captured public safety resources"—public safety personnel who work in other jurisdictions but cannot physically get there due to the damage—begin to check in at local fire houses and at the CCPD. Those who have their PSCDs with them are able to log into the local interoperability network and alert the EOC to their presence in Central City. The regional authentication database, housed at SLSD, provides authentication and privilege information as these personnel log in, and their location and personal information are added to the available personnel roster maintained by the logistics section at the city EOC. A similar process takes place within the county EOC for captured resources outside of the city, but within Santa Louisa County.

9. Pre-assigned members of the amateur radio community begin arriving at the EOCs and start staffing the amateur radio units located there. These RACES units provide logistical support to outlying agencies as well as communications support between an EOC and each of CCFD stations that have been designated as neighborhood emergency centers.

9:30 AM

10. Communications is established between the city and county EOCs, and with the SWC via the satellite system. The Governor, County Manager, Mayor and city and county emergency management directors are partied into a conference call via the very small aperture terminal (VSAT) system. Based on preliminary reports, the Governor directs his

staff to begin preparing a disaster declaration. Critical response information is passed to responding mutual aid personnel as they log into their local networks, and as they progress toward the scene through authenticated shared network access.

11. Field supervisors from CCPD begin arriving on scene at the major incidents, and assume the roles of local ICs. The assistant fire and police chiefs accompany the MCC to the field and assume overall IC responsibilities in a Unified Command structure, coordinating each of the individual sites. The ICs and communications unit leader, based on information being received from the field, set up the MCC in a location central to the major downtown high-rise collapses. In the MCC, the IC uses the PSCD to talk with the gas utility administrator and request the gas mains to city center be shut off. The IC requests that the DoT administrator as well as public works redirect traffic from the city center, and begin setting up an incident perimeter barrier that covers a 16-block area that allows only public safety traffic to enter. DoT uses ITS to reconfigure traffic signal lights, where connectivity and electrical power permit, and also to initiate warning messages to vehicle-mounted displays and VMSs along major roadways in surrounding areas in order to warn motorists to stay out of the incident zone. The IC makes additional resource requests to the EOC.

12. Two state police helicopters arrive in the area, and their video systems and FLIRs are linked to the MCC and the EOC. A general sweep of the area is initiated, allowing command staff to get an overall view; the video is recorded for later use.

13. The local jurisdiction's rescue and medical units are quickly being overwhelmed. The operations section chief requests assistance from several specialized US&R teams as well as CERTs.

14. Central City contacts the county EOC to request assistance from the county and state, including additional fire suppression resources, US&R task forces, and communications and logistics support. This request constitutes the formal activation of the state mutual aid system. One of the local US&R teams from the state Department of Forestry and Fire Protection (DFFP) is dispatched from Otsego and assigned to the search and rescue of victims in the two partially collapsed buildings. A DMAT from Capital City has been activated by the state, and a US&R Incident Support Team (IST)[3] is also deployed into the area. The state dispatches an OEM communications coordinator to the MCC to assess communications system integrity, and to coordinate DMAT and US&R communications resources. In anticipation of need, the OEM Communications Coordinator requests that a state OEM ICS type 1 communications unit and a trailer-mounted, high-capacity, satellite terminal be deployed to Central City.

15. Amateur radio operators communicating through the RACES communications unit at the county EOC have been reporting vegetation fires, damage to county roads and bridges, and rural residential damage in the county. The cities of Cooney, Fernwood, and Otsego report to the Santa Luisa County EOC via amateur radio and the county microwave voice and data network on conditions in their jurisdictions, and start requesting fire response, EMS, and public works resources.

10:45 AM

[3] The Incident Support Team (IST) supports US&R teams with tasking, material, and coordination.

16. Based on three-dimension geolocation information coming from the field, the logistics section chief uses the PSCD's city map monitor to show the locations of the reported damage, and displays command post and other critical information for EMS, fire response, police, and public works staff in the operations section. This allows the most appropriate selection of staging areas. The information is simultaneously transmitted to displays in the MCC.

17. The Governor activates National Guard units. The Governor also requests that Federal assistance, including national S&R teams and a Mobile Emergency Response System (MERS) unit, be sent to Central City.

11:00 AM

18. Using their PSCDs and the satellite network, a conference call takes place between the logistics chiefs at the MCC, in the Central City EOC, Santa Luisa County EOC, state EOC, and the US&R IST, and with the on-scene OEM communications coordinator. Decisions are made to establish a resource mobilization center at the Santa Luisa County Fairgrounds, to colocate the IST at the mobilization center, and to establish a unified communications resource coordination point. The OEM communications coordinator is designated to serve as the area communications coordinator. Using the vehicle-mounted satellite terminal in the Center City MCC, the OEM communications coordinator contacts the state EOC with a request for a DFFP communications unit leader, and a communications coordinator from the National Incident Radio Support Cache (NIRSC) to assist with the unified resource coordination. The OEM coordinator then orders that the OEM transportable satellite unit and the type 1 communications unit be set up at the fairgrounds, and requests that two caches, or 56 units, of OEM-owned PSCDs be staged at the mobilization center for potential use. A request for fuel trucks to support city and county facilities, particularly the EOCs, is issued.

11:30 AM

19. As reporting teams from the local and regional media arrive on the scene, the Central City PIO forms a JIC in a building adjacent to the EOC, and uses PSCDs to produce maps directing the placement of camera teams away from areas requiring unrestricted emergency access. The JIC will also provide press releases with supporting video and still imagery that will be made directly available to media data feeds using the capabilities of responder PSCDs. The JIC will distribute information to the public regarding the location of food, potable water, shelter, and operational waste disposal facilities.

20. Upon arrival at the collapsed building, the DFFP US&R unit sets up a base of operations at a safe distance from the building, as directed by the staging manager. Using their PSCDs, the US&R personnel begin surveying for structural integrity and for likely victim locations. Their PSCDs set up an IAN that links with the MCC database and obtains blueprints and building drawings. The node allows various voice, video, and data to be transmitted to similarly equipped units, including the IST and the DMAT. It also provides three-dimensional location information for all PSCD-equipped personnel that are plotted into a GIS-based tracking system. As units survey the scene, they are able to overlay

major structural displacements into the pre-event GIS database to allow improved structural analysis and determination of potential victim locations.

21. A CERT communication unit, an amateur radio operator, sets up in close proximity to the MCC and, working through the liaison officer, verifies a process to pass intelligence and logistics information from CERT to the US&R branch.

22. The Red Cross has set up a command post next to the MCC, and has activated shelters in several local schools. Red Cross personnel are capturing on their PSCDs the names of every person arriving at the shelters, and relaying the information to a central database that other parties can access. This information is available to the Red Cross representative in the EOC, as well as to key city officials. City public buses and public school buses, both of which operate on the public safety radio system, are alerted and organized to support transport of victims and the public to treatment facilities or shelters.

2:00 PM

23. The DMAT from Capital City has arrived and is setting up its unit. All patient names, medical conditions, etc. will be entered into PSCDs to track the earthquake victims. The SLSD coroner's unit begins setting up a central DMORT center for processing the dead, including collection of names and identifying information, as well as for the long-term storage of bodies. As bodies are brought to the collection point, critical data, including the location where they were found, are stored in a special central database.

24. CERT teams are becoming more organized as they search though residential areas for trapped victims. As they come across larger or more questionable structures, they request assistance from a US&R team as well as provide damage information through the CERT communications unit. PSCDs are linked to the city GIS system to log activities of these teams.

4:00 PM

25. Structural specialists begin the structural survey of the parking garage, using handheld PSCDs to sketch the structure perimeter, noting entrances and areas of structural concern. The survey data is wirelessly sent to the US&R's node where it is coordinated with pre-event GIS information. At the same time, a group of structural engineers begin looking over the drawing and blueprints for the buildings. Data collected indicates that a larger building is on the verge of collapse within the next 24 hours. This information is relayed to all public safety units via the PSCDs, and to the command post established at the park. This information is then transmitted to the IC, who can make entry plans from this data. Using this data, IC establishes the hazard zone for tracking entry into the garage and the collapsing building. At the same time, the data is relayed from the MCC through the satellite network to the IST at the mobilization center to assist in its long-range planning.

26. The structural specialists find that one outside wall of the parking garage has fallen away and the concrete T-bars of the parking garage have detached from the outside wall, collapsing it. The engineering team at the Federal building finds that a gas main on the north side of the building was ruptured, with leaking and trapped gas posing an explosion hazard. The gas utility representative in the EOC is requested to ensure that gas mains are off and, where the gas valve control system may have failed, that dispatch personnel

manually check and secure valves. The police are directed to cordon off a four-square-block area and begin necessary evacuations. The structural specialists set up two theodolites[11] to monitor any movement of the Federal building. These units contain video cameras that transmit images via an integrated broadband transmitter to the base of operations, where the specialists can safely monitor the structure. Once a preliminary structural assessment is complete, the IC assigns the search teams to enter the structure to search for victims. The teams are assisted by hazardous materials (Hazmat) specialists, who detect any nuclear, biological, or chemical hazards to the rescue personnel. A search of the appropriate databases allows for an inventory of the building contents to be reviewed, examined, and the results transmitted to all officials involved.

27. Two search teams that will enter the garage area and Federal building turn on their personal safety systems, which include activity monitor and three-dimensional location tracking systems. As the teams enter the hazard zone, they check in with a safety officer, who notes their entry using a PSCD. This information is used at the base of operations to track all personnel inside the hazard zone. As the search teams search, they note the presence or absence of victims on their PSCDs, and the data is displayed on the floor plan of the structure at the base of operations. As the teams move through the garage, the locations of all team members are logged for use if a member becomes lost or incapacitated.

28. The Hazmat Team links its hand-held monitoring equipment into a PSCD, which relays any detection information to a safety officer's terminal at the MCC. As search team 2 proceeds into the parking garage, the Hazmat team detects a potentially dangerous level of gasoline vapor in the air. A safety officer's instrument indicates the danger, and he decides that this route into the garage is too hazardous. He orders the team out of the garage, and to find another entrance. Before the team exits, they leave a remote combustible gas detector. This terminal will continuously monitor the air and, if an explosive condition is detected, will send an evacuation signal to all personnel in the structure.

29. Search team 2 uses their voice radios and PSCDs to coordinate their search, and the search team leader uses his PSCD to report the team’s progress to the IC. Team 2 locates several victims trapped in vehicles under the concrete T-bar sections, and notes their locations on the PSCDs. The IC calls for a rescue team to go to the garage to assist in the rescue operation. Rescue team 1 begins work on the extrication of the victims. As the rescue team accesses each patient, medical specialists treat the patient as much as possible in the confined space.

30. The medical team managers use their PSCDs at the base of operations to inform the IST and the DMAT of the number of victims, the severity of their injuries, and the estimated time of their extrication. When it is decided that one of the victims requires a leg amputation before extrication, the medical specialists consult with the medical team managers using voice and video exchange with their PSCDs.

31. Due to the number of victims in the immediate area, the demand for communications exceeds the available capabilities. The PSCDs execute prioritization routines that prioritize communications based on need. Voice communications are given top priority, vital medical data is given second priority, medical video data is scaled back to fewer

frames per second, and on-scene medical personnel prioritize individual cases so that video is periodically dropped for lower-priority patients.

6:00 PM

32. The IC, safety officer, and operation section chief use data on the total time each team has been in the structure to rotate teams for rest and rehabilitation. Eventually, all victims in the garage are extricated, stabilized, and transported to the DMAT. The IC then contacts the logistics section chief for re-supply of expended equipment and material, and discusses priorities and the team's next assignments with the planning section chief.

33. National Guard units activated by the Governor begin arriving. These units are seamlessly integrated into the communications network using their own PSCDs.

9:00 PM

34. A Federal US&R task force, flown by military air transport to Cooney Regional Airport, arrives to support the ongoing effort. Its voice and data PSCDs are entered into the regional authentication database and the communications unit leader authorizes their participation. They join the incident's network. The task force's leader uses his PWD to send the personnel and equipment manifests to the IST at the mobilization center. The task force uses robotic units capable of remotely providing video, audio, and sensing information from inside the building. The units transmit their information to the US&R incident base.

Transmission History

Though not reiterated in the following table, note that the transmission IDs a2 and a3 are repeated numerous times during the course of the scenario as teams check the structural integrity of key facilities in the area.

Table 1: Transmission Record Earthquake Scenario

Time: ID:	Response: PSAP, EOC, Police, Fire, EMS, Other:	Transmission Type:	State Agency Participation
Time: 9:02 ID: a1	PSAP: Fire and building inspectors dispatched to PSAP Fire: Dispatched to PSAP Other: Building inspectors dispatched to PSAP	Transmission Type: Binary (Fire), Voice (Inspectors)	
Time: 9:02 ID: a2	Other: Building inspectors download building plans	Transmission Type: Binary	
Time: 9:02 ID: a3	Fire: IAN established for firefighters and building inspectors at PSAP building Other: IAN established for firefighters and building inspectors at PSAP building	Transmission Type: Voice, Binary	
Time: 9:02 ID: a4	EOC: City/county EOC activated and key staff alerted	Transmission Type: Binary, Text	
Time: 9:02 ID: a5	EOC: Incident area network established for key staff (emergency manager, mayor, county exec, etc.) enroute to Operations Center	Transmission Type: Voice	
Time: 9:02	EOC: Callback of off-duty workers	Transmission Type:	

Time: ID:	Response: PSAP, EOC, Police, Fire, EMS, Other:	Transmission Type:	State Agency Participation
ID: a6		Binary	
Time: 9:02 ID: b1	EOC: State EOC activated; SWC automatically notifies state personnel	Transmission Type: Text	
Time: 9:02 ID: b2	EOC: SWC notifies surrounding counties	Transmission Type: Text	
Time: 9:02 ID: b3	EOC: SWC notifies NAWAS	Transmission Type: Binary via Wire-Based Tie Line	
Time: 9:02 ID: b4	EOC: FEMA regional and national Operations Centers begin alerting of disaster personnel across the country	Transmission Type: Binary via Wire-Based Tie Line	
Time: 9:02 ID: b5	EOC: SWC operator notifies governor's staff, key legislators, state agency heads	Transmission Type: Voice via Telephone	
Time: 9:10 ID: c1	PSAP: Continuous incoming calls		
Time: 9:10 ID: d1	PSAP: Dispatch police, fire, and EMS Police: Units dispatched to area Fire: Units dispatched to area EMS: Units dispatched to area	Transmission Type: Binary	
Time: 9:10 ID: d2	Fire: Fire units report locations of structure fires	Transmission Type: Binary	
Time: 9:10 ID: d3	PSAP: Receives request for preliminary damage assessment EOC: SWC sends request for preliminary damage assessment	Transmission Type: Binary via VSAT	
Time: 9:15 ID: e1	EOC: Emergency managers and key city and county staff arrive; as they arrive on scene they are removed from temporary net		
Time: 9:20 ID: f1	Police: Police, fire response, and EMS begin arriving at various scenes; at each scene an IAN is established for all first responders on scene	Transmission Type: Voice	
Time: 9:20 ID: f2	EMS: EMS units begin transporting victims to hospitals; patient vital signs relayed to hospitals; status information relayed to EOC	Transmission Type: Voice, Binary	
Time: 9:20 ID: g1	Other: RACES sets up at EOC, fire stations, and outlying agencies	Transmission Type: Voice, Binary	
Time: 9:20 ID: h1	EOC: User group established between city/county EOC, SWC, and Governor's office	Transmission Type: Voice via VSAT	
Time: 9:30 ID: i1	Police: Field supervisors beginning to arrive at scenes, establish IC Fire: MCC deployed at scene of building collapse; user group established linking site commanders, MCC, and EOC	Transmission Type: Voice	
Time: 9:30 ID: i2	Police: User group established linking on-scene commanders to EOC Fire: User group established linking on-scene commanders to EOC	Transmission Type: Voice	
Time: 9:30 ID: i3	Police: As first responders arrive at each scene, register electronically to be added to on-scene roster	Transmission Type: Binary	

Time: ID:	Response: PSAP, EOC, Police, Fire, EMS, Other:	Transmission Type:	State Agency Participation
	and included in incident area network		
Time: 9:30 ID: i4	Police: State police helicopters sent to area to perform aerial reconnaissance; video linked to EOC and MCC; pilots added to temporary net for command	Transmission Type: Video, Voice	
Time: 9:30 ID: i5	Fire: Overall IC contacts gas utility to shut off gas mains to city center	Transmission Type: Voice	
Time: 9:30 ID: i6	Fire: IC contacts city DPW to redirect traffic and establish barricades	Transmission Type: Voice	
Time: 9:30 ID: j1	Fire: Operations Section Chief requests US&R and CERT	Transmission Type: Voice	
Time: 9:30 ID: k1	EOC: Mayor requests state US&R and DMAT teams	Transmission Type: Voice via Telephone	
Time: 9:30 ID: k2	EOC: State dispatches OEM Communications capability to Central City with reach back capability to state OEM	Transmission Type: Voice, Binary, Image, Video via Infrastructure, VSAT	
Time: 9:30 ID: l1	Other: RACES operators report damage outside Central City and relay requests for assistance form outlying cities	Transmission Type: Voice, Binary	
Time: 10:45 ID: m1	EOC: Display shows location of units (from reported three-dimensional geolocation), damage reports on map; information used to select staging areas Fire: Display shows location of units (from reported three-dimensional geolocation), damage reports on map	Transmission Type: Binary (Three-Dimensional	
Time: 11:00 ID: n1	EOC: Governor activates National Guard, requests national US&R and MERS assistance		
Time: 11:00 ID: o1	EOC: Conference call	Transmission Type: Voice via VSAT	
Time: 11:30 ID: p1	Fire: PIO uses location and damage information for placement of media teams, generates video and images that are transmitted electronically to media representatives	Transmission Type: Binary, Image, Video	
Time: 11:30 ID: q1	Other: DFFP US&R arrives, added to IAN; tactical user group also established		
Time: 11:30 ID: q2	Other: Short-range broadband net established to relay video, marked-up blueprints, and images among IC members		
Time: 11:30 ID: r1	Fire: CERT communication team sets up link to US&R	Transmission Type: Binary, Image, Video	
Time: 11:30 ID: s1	Other: Red Cross sets up emergency shelters; user group to link Red Cross representatives with EOC; link used to exchange data on survivors, status	Transmission Type: Voice, Binary	
Time: 14:00 ID: t1	EMS: DMAT deploys; links to EOC Medical Coordinator and hospitals to exchange victim data; DMAT commander added to command network	Transmission Type: Voice, Binary	

Time: ID:	Response: PSAP, EOC, Police, Fire, EMS, Other:	Transmission Type:	State Agency Participation
Time: 14:00 ID: u1	Other: CERT team commanders are linked in a user group with EOC; when necessary linked into US&R temporary net as well		
Time: 16:00 ID: v1	Other: Structural specialists are linked into US&R IAN	Transmission Type: Voice, Binary	
Time: 16:00 ID: v2	EOC: Structural data is overlaid with blueprint information		
Time: 16:00 ID: v3	EOC: Structure risk broadcast to all units	Transmission Type: Voice, Binary	
Time: 16:00 ID: v4	Fire: IC establishes hazard zone, requests barricades from Central City DPW streets maintenance to establish perimeter	Transmission Type: Voice	
Time: 16:00 ID: w1	Other: team informs IC of ruptured gas line	Transmission Type: Voice	
Time: 16:00 ID: w2	Fire: IC directs police to establish perimeter area around gas	Transmission Type: Voice	
Time: 16:00 ID: w3	Other: Structural specialists set up theodolites	Transmission Type: Binary, Video	
Time: 16:00 ID: w4	Fire: Hazmat team queries database to identify any potential hazards in building	Transmission Type: Binary	
Time: 16:00 ID: w5	Other: Structural specialists verify structural integrity	Transmission Type: Voice	
Time: 16:00 ID: w6	Fire: IC directs search and Hazmat teams to enter building to search for victims; incident area network for personnel in building established	Transmission Type: Voice	
Time: 16:00 ID: x1	Other: Search teams entering garage area establish IAN for activity monitoring and location information; data (such as location and status of victims) is also transmitted	Transmission Type: Binary	
Time: 16:00 ID: y1	Fire: Hazmat team links monitoring equipment to communications network; information transmitted to on-scene commander and MCC	Transmission Type: Binary	
Time: 16:00 ID: y2	Fire: Units ordered out from structure	Transmission Type: Voice	
Time: 16:00 ID: y3	Fire: Units leave behind remote monitor	Transmission Type: Binary	
Time: 16:00 ID: z1	Other: Search teams continue searching garage	Transmission Type: Voice, binary	
Time: 16:00 ID: z2	EMS: Rescue team attends to victims; medical status and video transmitted to hospitals; due to data exceeding available bandwidth, degraded bandwidth management is in effect	Transmission Type: Voice, Binary, Video	
Time: 18:00 ID: aa1	EOC: IC staff uses activity data to rest and rotate search and rescue teams	Transmission Type: Voice, Binary	
Time: 18:00 ID: bb1	Other: National Guard begins arriving; command added to command network; officers added to IAN at specific scenes where they are working with first responders	Transmission Type: Voice, Binary	

Time: ID:	Response: PSAP, EOC, Police, Fire, EMS, Other:	Transmission Type:	State Agency Participation
Time: 21:00 ID: cc1	Other: Federal US&R team arrives; command network added; unit personnel added to on-scene responder rosters; robotic unit deployed with short-range communication for transmitting video from inside collapsed buildings; video transmitted when requested to MCC and EOC	Transmission Type: Voice, Binary, Video	

ATTACHMENT “D”

5 System of Systems

This section describes, in detail, the network topology that will be used in meeting the requirements set forth in Section 6, Section 7, and Section 8. Specifically, this section defines the network interfaces, both wired and wireless, and defines the links between the interfaces.

5.1 Network Description

The communications systems must be integrated with the public safety user's operations. For example, as a police officer leaves a patrol car to respond to a traffic stop or to investigate a domestic dispute, the critical communications capabilities, whether voice or data, must remain with the officer. As a firefighter enters a burning building, the biometric monitoring devices, the equipment status devices, and the firefighter's location device must indicate to the IC the firefighter's status and location at all times. These wireless devices must work in a variety of networks. Together, they will form the system of systems (see Figure 1).

They will have the following natural network hierarchy.

a. **PAN**—The PAN for a first responder can take on many different forms. Primarily, it is intended to represent a set of devices on the person of a first responder that communicate with the first responder’s PSCD as necessary. The devices on a PAN will include such items as heart rate monitors, location sensors, etc. This information could, and would in many cases, be transmitted to other areas of the network.

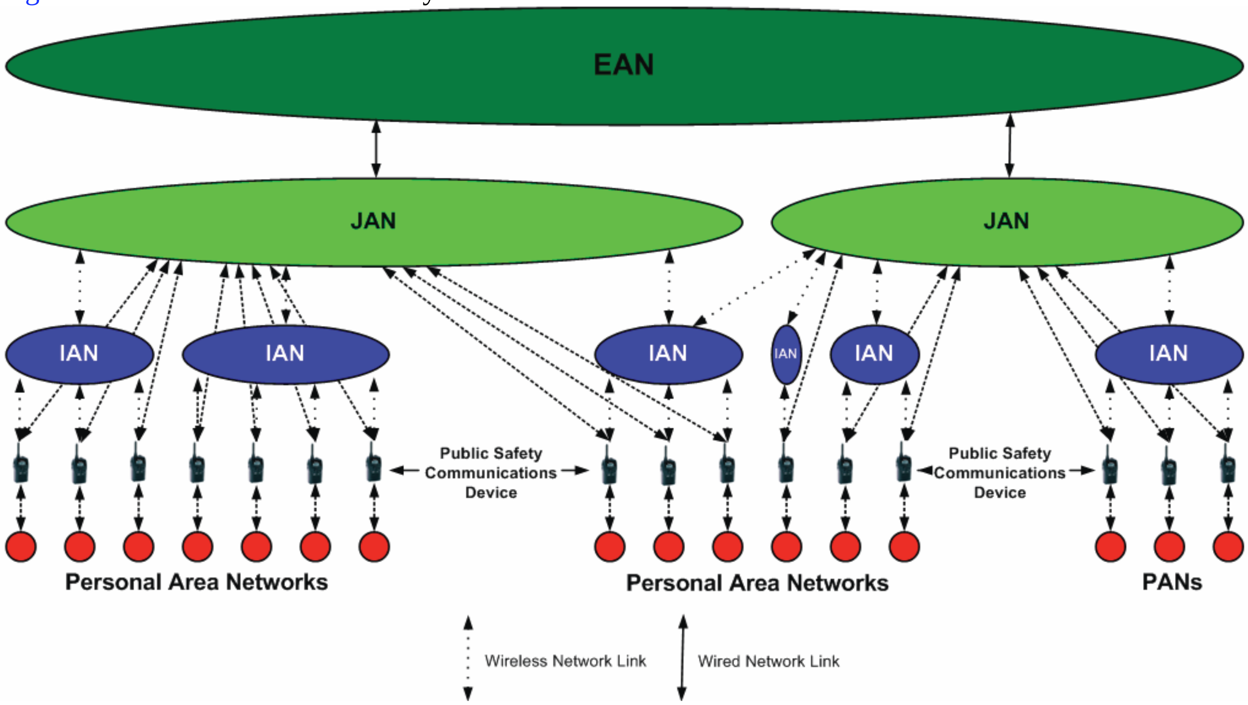
b. **IAN**—An IAN is a network created for a specific incident. This network is temporary in nature; it is typically centered on a wireless access point attached to the first responders’ vehicle, or an IAN node. Multiple vehicles therefore dictate multiple nodes, all of which coordinate their coverage and transmissions seamlessly and automatically. This network scales to the size of the incident, from a local traffic stop, to a large-scale, multi-discipline, multi-jurisdiction event. Thus, when an incident is dispersed across a large geographic area, it is expected that the IAN will also leverage the JANs and EANs as needed.

c. **JAN**—The JAN is the main communications network for first responders. It handles any IAN traffic that needs access to the general network, and provides the connectivity to the EAN. This network is more permanent in nature, and is typically made up of JAN nodes, or communications towers. Additionally, it is the component of the network that will handle any and all communications from a first responder’s PSCD, should a connection with the local IAN fail or be otherwise unavailable.

d. **EAN**—The local systems are, in turn, linked with county, regional, state, and national systems or EANs. It is expected that this network could be both wired and wireless, depending on the type of infrastructure deployed in the area, e.g., microwave point-to-point, fiber.

Each of the area networks described above are logical concepts. This is an important point to make, as an IAN can be made up of both IAN nodes as well as JAN nodes. Conversely, a JAN can be made up of JAN nodes in addition to an EAN link to connect geographically diverse JAN nodes. This concept is explored further in Section 5.3.

Figure 1: Natural Network Hierarchy



Because public safety operations are usually conducted in the field and emergency operations must take place in the vicinity of the emergency, the networks must allow for mobile members and/or the networks themselves must be mobile and temporary in nature. They must be dynamic and scalable to allow new resources to come onto a temporary network, and they must allow temporary networks to integrate with larger temporary or fixed networks.

Additionally, the management of these networks must allow for automated management as well as user-led management, when necessary and as local policy dictates.

5.2 Network Diagram

The following network diagram shows all of the links and interfaces that have been identified at this point
based on the scenarios and requirements discussed in this document.

Figure 2: Link Diagram

In the preceding figure, the dotted lines denote a wireless connection, and the solid lines denote a wired or wireless connection. A red circle around the end of a link denotes a distinct interface, whether wired or wireless.

The following table provides a short description of each link.

Table 29: Network Diagram Link Descriptions

Link	Represents the Connection Between
Link 1	The PAN of the first responder and the first responder's PSCD. The data collected by the sensors on the first responder's body is transmitted aggregately to the PSCD. The main considerations in sizing this link are the amount of data to be transmitted, the distance the transmission must travel, and interference from outside sources, including other first responders' PANs.
Link 2	The first responder's PSCD and the first responder vehicle (FRV) when the PSCD is in range of the vehicle's node, creating part or all of the IAN. Links 2, 3, and 4 all use the same interface, but separating the links allows for separate performance specifications for each.
Link 3	PSCD to PSCD communications. This link is used in peer-to-peer communications. Links 2, 3, and 4 all use the same interface, but separating the links allows for separate performance specifications for each.
Link 4	FRV-to-FRV communications. Links 2, 3, and 4 all use the same interface, but separating the links allows for separate performance specifications for each.
Link 5	The first responder's PSCD and JAN infrastructure. This connection is only used when the first responder is out of range of an IAN node created by an FRV node or some other IAN node. This means a first responder on foot would use this link all the time, while a first responder operating out of a vehicle would only use this link when the connection between the first responder's PSCD and the vehicle IAN node were unavailable.
Link 6	The FRV and the JAN infrastructure. This link is used for the same traffic that link 5 is used for, the primary differentiator being the location of the first responder with respect to an FRV. As was described for link 5, if the first responder is within transmission distance of the vehicle node, data is passed over the vehicle IAN node before being transmitted to the JAN node; otherwise, the first responder's PSCD transmits directly to the JAN node.
Link 7	The JAN infrastructure pieces. While this connection is most likely also connected to the dispatch central office, it provides the capability to describe traffic that does not route itself through the dispatch central office.
Link 8	The dispatch central office and JAN infrastructure.
Link 9	The dispatch central office and a wider network. It is through this link that DMV, NCIC, PSTN, and other extranet queries will be forwarded.
Link 10	This link denotes FRV-to-vehicle communications over the JAN interface without passing through a JAN tower node. In other words, this link accommodates ad hoc networking using the JAN interface.

Each of the interfaces identified in Figure 2 is unique to the network. The following table provides a short description for each interface.

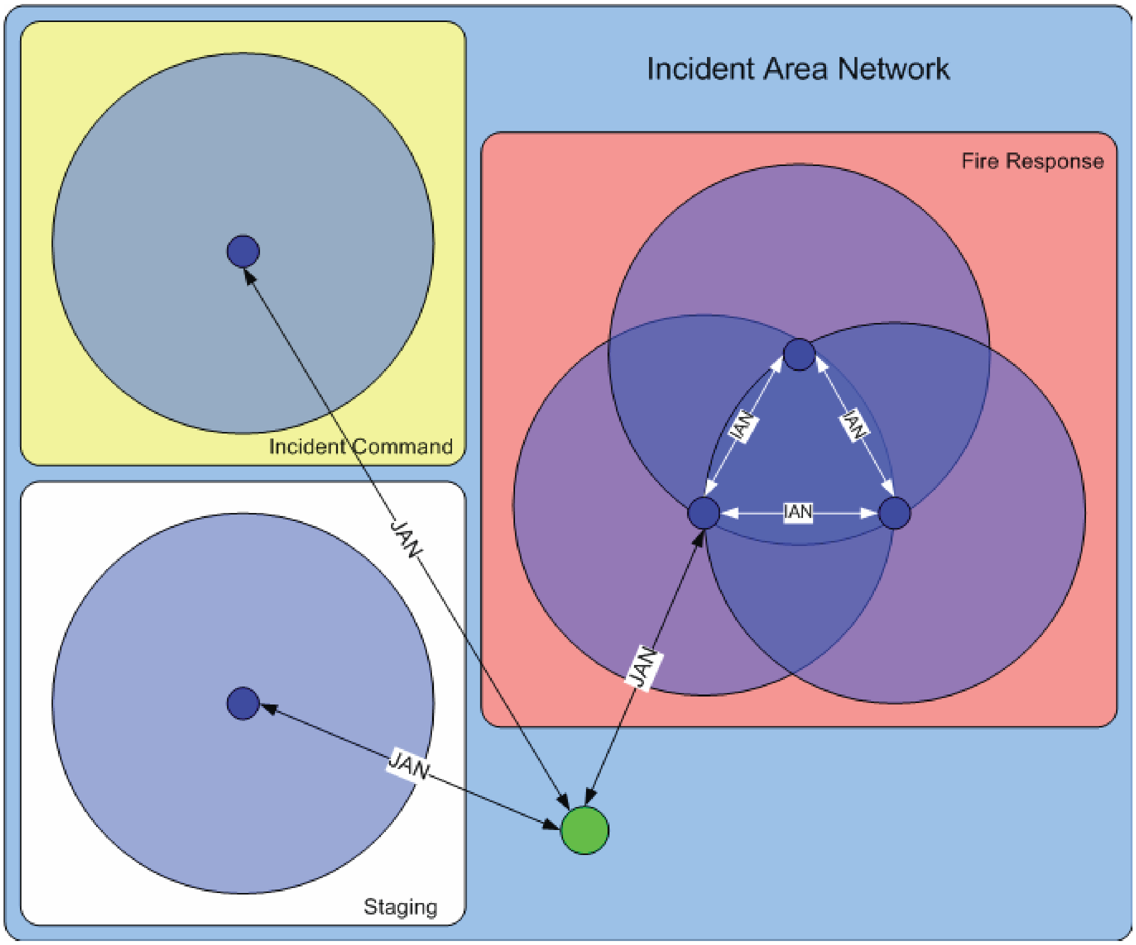
Table 30: Network Diagram Interface Descriptions

Interface	Is Specified As
Interface 1	The interface that handles the aggregate transmissions to or from a first responder's PAN to or from the PSCD. This is a wireless interface unless the PSCD is integrated directly into the PAN.
Interface 2	The interface that handles transmission to or from the PSCD/FRV to or from the PSCD/FRV via the IAN. This is a wireless interface.
Interface 3	The interface that handles transmissions to or from the PSCD/FRV to or from the fixed/mobile infrastructure via the JAN. This interface also accommodates FRV-to-FRV communications as needs dictate. This is a wireless interface.
Interface 4	The interface on a piece of fixed/mobile infrastructure that handles transmissions to or from another piece of fixed/mobile infrastructure. This interface can be wired or wireless.
Interface 5	The interface that handles transmissions to or from a piece of fixed/mobile infrastructure to or from the local dispatch central office. This interface can be wired or wireless.
Interface 6	The interface to or from other network types, including the PSTN, other jurisdictions, the public Internet, and so forth to or from the dispatch central office. This is a wired interface.

5.3 Network Topology

The four area networks (PAN, IAN, JAN, and EAN) discussed in Section 5.1 are logical constructs that provide context for understanding different aspects of a public safety communications network. Each area network type is created using nodes. For example, an IAN can be created using a grouping of IAN nodes on first responder vehicles. The PAN is a combination of devices on the person of a first responder. The JAN will most likely be constructed from JAN nodes on towers, akin to today's LMR towers. And while these examples are the likely cases, they are not intended to be limiting. Using the scenario Section 3.5 describes, Figure 3 and Figure 4 show two IAN examples to further describe the flexibility of the network hierarchy that Figure 1 presents.

Figure 3: Incident Area Network with JAN Tower Node



In Figure 3, the smaller dark blue circles indicate IAN nodes. These nodes are notionally placed on top of FRVs. The larger light blue circles indicate coverage for the IAN nodes on the vehicles. The light green circle indicates a JAN tower node. The three boxes indicate geographically diverse areas for the scenario.
As shown, the light yellow box denotes the location of Incident Command, the white box showing the staging area as separate from Incident Command, while the light red box shows the first response area. As indicated, the black arrows denote a JAN communications link while the white arrows denote an IAN communications link.

The three boxes indicate geographically diverse areas for the scenario. As shown, the light yellow box denotes the location of incident command, the white box showing the staging area as separate from incident command, while the light red box shows the first response area. As indicated, the black arrows denote a JAN communications link, while the white arrows denote an IAN communications link.

Based on the diagram, the light blue box shows the logical IAN that is created to combat a chemical plant explosion. It is a logical description because there are three groups of IAN nodes that are connected together through a JAN tower node that is acting as a notional repeater in addition to providing backhaul to the rest of the communications network as needed. So, in this example, the IAN includes three separate groups of IAN nodes connected together via a JAN tower node.

Figure 4: Incident Area Network without a JAN Tower

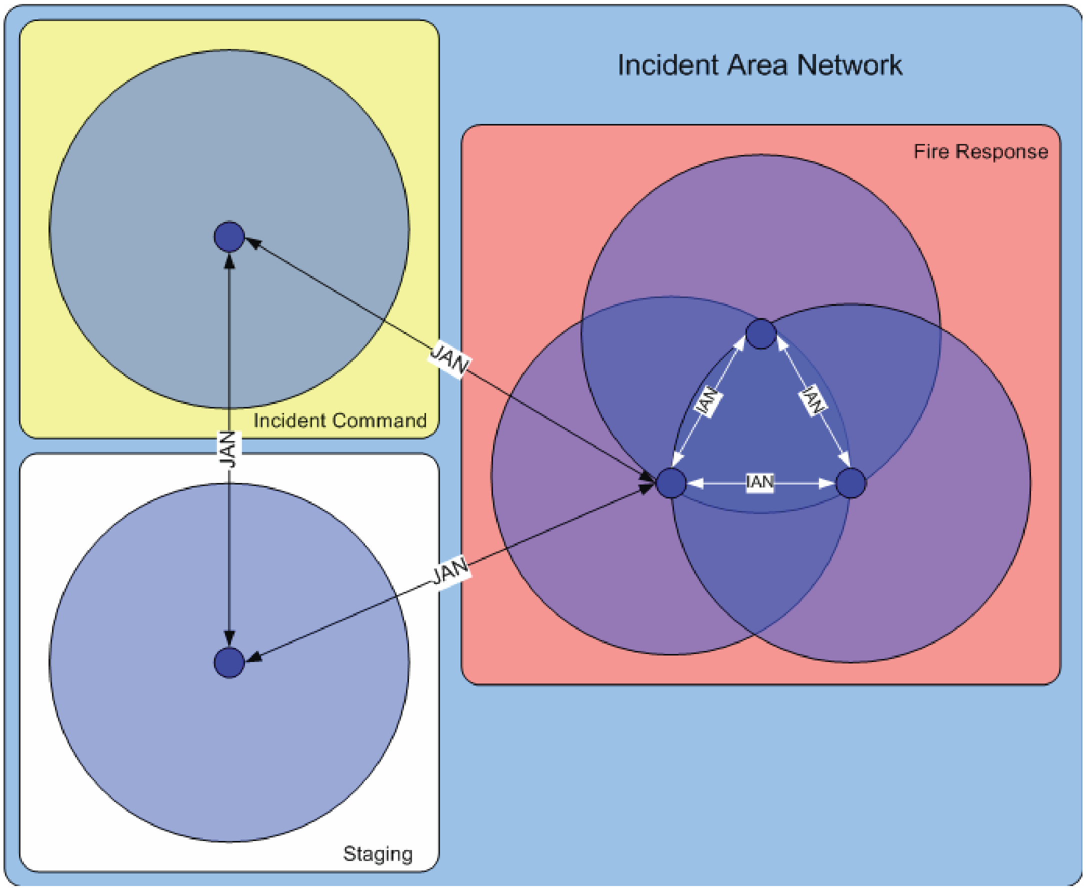


Figure 4 is similar to Figure 3, but lacks a JAN tower node. Figure 4 shows that, in the absence of a JAN tower node to act as a repeater connecting the three IAN node clusters, the JAN interfaces on the vehicle can create an ad hoc network amongst themselves to relay traffic to and from the three areas of the incident.